Department of Homeland Security

Office of Inspector General

Transportation Security Administration's Deployment and Use of Advanced Imaging Technology

OIG-13-120

September 2013

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

SEP 16 2013

MEMORANDUM FOR: John W. Halinski
Deputy Administrator
Transportation Security Administration

FROM: Anne L. Richards
Assistant Inspector General for Audits

SUBJECT: *Transportation Security Administration's Deployment and Use of Advanced Imaging Technology*

Attached for your information is our final report, *Transportation Security Administration's Deployment and Use of Advanced Imaging Technology*. We incorporated the formal comments from the Transportation Security Administration in the final report.

The report contains two recommendations aimed at improving the deployment and use of advanced imaging technology. Your office concurred with both recommendations. However, TSA's response did not include steps to implement the recommendations. As prescribed by the *Department of Homeland Security Directive 077-01, Follow-Up and Resolutions for Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation.

Please email a signed PDF copy of all responses and closeout requests to OIGAuditsFollowup@oig.dhs.gov. Until your response to the recommendations is received and evaluated, the recommendations will be considered open and unresolved.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Mark Bell, Deputy Assistant Inspector General for Audits, at (202) 254-4100.

Attachment

Table of Contents

Appendixes

Abbreviations

AIT	advanced imaging technology
DHS	Department of Homeland Security
GAGAS	generally accepted government auditing standards
OIG	Office of Inspector General
PMIS	Performance Measurement Information System
TSA	Transportation Security Administration
TSO	Transportation Security Officer

Executive Summary

The Transportation Security Administration (TSA) secures the nation's airports and screens commercial airline passengers and baggage. It uses advanced imaging technology to screen passengers for metallic and nonmetallic threats, including weapons, explosives, and other concealed objects, without physical contact.

TSA began deploying advanced imaging technology in 2007 and accelerated its deployment after the attempted airplane bombing on December 25, 2009. In 2012, Representative John Mica requested that the Department of Homeland Security (DHS) Office of Inspector General (OIG) conduct an audit to determine whether TSA is effectively deploying advanced imaging technology and is fully utilizing the equipment at airports.

TSA created and followed deployment schedules. However, it did not develop a comprehensive deployment strategy to ensure all advanced imaging technology units were effectively deployed and fully used for screening passengers. This condition existed because TSA did not—

- Have a policy or process requiring program offices to prepare strategic deployment plans for new technology that align with the overall goals of the Passenger Screening Program, and
- Have adequate internal controls to ensure accurate data on advanced imaging technology utilization.

Without a documented, approved, comprehensive plan and accurate data on the use of advanced imaging technology, TSA continued to use walkthrough metal detectors, which are unable to identify non-metallic objects, to screen the majority of passengers; therefore not taking advantage of the advanced imaging technology's security benefits. Additionally, TSA may have used resources inefficiently to purchase and deploy underused advanced imaging technology units.

We made two recommendations to improve the effectiveness of how TSA deploys and measures the use of advanced imaging technology. TSA concurred with both recommendations.

Background

TSA was created to strengthen the security of the nation's transportation systems and ensure the freedom of movement for people and commerce. TSA is responsible for conducting checkpoint screening operations at federalized airports. Its mission is to conduct screening operations in a manner that maximizes passenger throughput and threat detection while alleviating privacy concerns. Within TSA, the Passenger Screening Program is responsible for providing technology to screen passengers and carry-on baggage at airport security checkpoints.

Historically, TSA used walkthrough metal detectors to screen passengers at airport security checkpoints. As the threat to transportation security evolved, TSA needed a screening technology to detect nonmetallic threats. Advanced imaging technology (AIT) screens passengers for metallic and nonmetallic threats, including weapons, explosives, and other concealed objects, without physical contact. TSA began deploying AIT in 2007 and accelerated its deployment after the attempted airplane bombing on December 25, 2009.[1]

Types of AIT

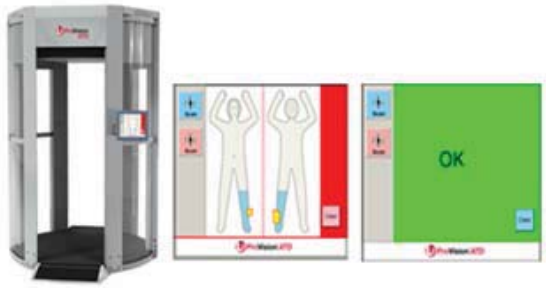
Millimeter wave technology uses electromagnetic waves to create the same generic image for all passengers.

Backscatter technology projects low-level X-ray beams over the body to create a reflection of the body displayed on the monitor.

Source: TSA.

TSA deployed AIT with millimeter wave and backscatter technologies. Both types of AIT create an image of a passenger's body that identifies items not readily visible. Initial AIT units required a Transportation Security Officer (TSO) to review and interpret the images, generating privacy concerns among travelers and members of Congress.

Figure 1: AIT with Automated Target Recognition



Source: L3 Communications.

In 2011, TSA added automatic target recognition software to the millimeter wave AIT. Automatic target recognition software addresses privacy concerns by interpreting images and displaying the results on a generic figure, as shown in figure 1. The *FAA Modernization and Reform Act of 2012* mandated that, beginning

[1] Northwest Airlines flight 253 was the target of a failed Al-Qaeda bombing attempt.

June 2012, TSA shall ensure AIT used for passenger screening is equipped with automatic recognition software. The TSA Administrator issued a waiver extending the deadline to June 1, 2013.

As of January 2013, TSA had purchased 997 AIT units at a total cost of approximately $150 million. Table 1 provides a summary of the total cost of all AIT units purchased.

Table 1: Cost of AIT Units Purchased

Type	Unit Cost	Cost of AITs by Type	No. of AIT Units Purchased
Millimeter Wave AIT	$148,200	$110,557,200	746
Backscatter AIT	$159,584	40,055,584	251
Total		**$150,612,784**	**997**

Source: OIG analysis of TSA data.

In January 2013, TSA decided to remove all backscatter AIT units from airports because these units would not meet the June 2013 deadline to comply with the *FAA Modernization and Reform Act of 2012*. This affected 251 units purchased for approximately $40 million.

TSA uses passenger throughput data entered into the Performance Measurement Information System (PMIS) to measure the use of AIT. TSA extracts data from PMIS to provide throughput information to airport Federal Security Directors and TSA leadership to assist in managing operations. TSOs manually collect and enter passenger checkpoint throughput data (such as AIT and walkthrough metal detector throughput) into PMIS. TSA has not performed a reliability assessment on AIT throughput data recorded in PMIS.

Representative John Mica, Chairman, Subcommittee on Government Operations, Committee on Oversight and Government Reform requested this audit in January 2012. Representative Mica expressed concern about TSA purchasing and deploying AIT units that it is not using at the airports. [2] This report responds to his request. Our objective, scope, and methodology are provided in appendix A.

[2] Representative Mica requested this audit during the last congressional term where he served as Chairman of the House Transportation and Infrastructure Committee.

Results of Audit

TSA created and followed deployment schedules showing the order in which airports would receive AIT units. However, it did not develop a comprehensive deployment strategy to ensure all AIT units were effectively deployed and fully used for screening passengers. This condition existed because TSA did not—

- Have a policy or process requiring program offices to prepare strategic deployment plans for new technology that align with the overall goals of the Passenger Screening Program, and
- Have adequate internal controls to ensure accurate data on AIT utilization.

Without a documented, approved, comprehensive plan and accurate data on the use of advanced imaging technology, TSA continued to use walkthrough metal detectors, which are unable to identify non-metallic objects, to screen the majority of passengers; therefore not taking advantage of the advanced imaging technology's security benefits. Additionally, TSA may have used resources inefficiently to purchase and deploy underused AIT units.

Strategic Deployment Planning

TSA did not develop a strategic deployment planning document to address the introduction and use of AIT to screen passengers at airports. Rather than develop a comprehensive strategic deployment plan, TSA created documents and schedules with short term goals based on institutional knowledge to deploy AIT. Documents that TSA provided contained inconsistent information or were not signed by senior leadership, creating doubt as to whether the documents were ever approved. In addition, TSA did not have a policy or process requiring program offices to document strategic deployment plans for new technology that align with the goals of the Passenger Screening Program. Without a documented, approved, comprehensive strategic deployment plan to address short- and long-term goals, TSA may have inefficiently used resources to purchase and deploy underused AIT units.

Deployment Planning Documents

TSA created and followed deployment schedules and documents identifying short term goals, but did not develop a comprehensive strategic deployment plan. A strategic deployment plan would provide TSA a baseline to respond to and plan for evolving threats, goals, and priorities. TSA and DHS do not have specific policies or procedures for developing or documenting deployment plans.

An effective strategic deployment plan should include the purpose and description, identify necessary tasks, define roles and responsibilities, identify logistics requirements, document site selection methodology and deployment schedule, and outline disposal plans.

TSA created deployment schedules that documented the order in which airports would receive AIT units. TSA based the deployment schedules on the following three priorities:

- High threat airports with available Transportation Security Officers,
- AIT pilot locations, and
- Highest threat airports.

TSA also considered airport size and available space, but not as a separate factor. TSA measured the airport's screening area dimensions (i.e., ceiling height, lane width) to ensure AIT units could fit the space before including an airport on the deployment schedule. These documents did not show how or to what extent TSA aligned AIT deployment with the overall goals of the Passenger Screening Program.

Additionally, TSA deployed AIT using information contained in various documents that were fragmented and developed independently from one another. Some documents contained inconsistent information and were unsigned and undated, and provided no evidence of TSA's senior leadership approval. TSA had difficulty providing historical information as well. TSA could not provide strategic deployment planning documents created before 2010; yet the component deployed an AIT unit at the Phoenix Sky Harbor International Airport in 2007. Strategic planning is important for a successful deployment of screening technology. Without a comprehensive, strategic deployment plan and a process for approving changes to the plan, TSA decision makers do not have a systematic approach to maximizing technology advances for reducing current and evolving threats. Moreover, the absence of a comprehensive strategy to deploy AIT units may lead to underused AIT units at airports, possibly inefficiently using resources to purchase and deploy underused AIT units, and reducing the security benefits of AIT by continuing to use walkthrough metal detectors to screen passengers.

Actions Taken During the Audit

TSA officials recognized the benefits of developing and maintaining a strategic deployment plan for its passenger screening equipment and began drafting a comprehensive deployment strategy in July 2012. TSA drafted two separate

documents—one to provide a historical record of AIT deployment; the second to provide a deployment strategy for all Passenger Screening Program equipment. As of April 2013, the documents were still in draft. A comprehensive, strategic deployment plan defining deployment goals may eliminate or minimize problems in future equipment deployments.

Data Reliability

TSA did not have adequate internal controls to ensure accurate data on AIT use. We assessed PMIS data in accordance with the Government Accountability Office's guidance, *Assessing the Reliability of Computer-Processed Data*.[3] We could not determine the reliability of PMIS data used to report AIT use because—

- PMIS application and quality controls were not sufficient to identify and correct potential errors;
- Airports discarded original source documents, preventing us from reconciling the information; and
- PMIS and airport source documents during limited validation testing for a 10-day timeframe for five category X airports were inconsistent.[4]

PMIS Application Controls

PMIS application controls did not ensure airports reported accurate passenger throughput data to TSA headquarters. The Government Accountability Office defines application controls as internal controls incorporated directly into computer applications to help ensure the validity, completeness, accuracy, and confidentiality of transactions. Application controls include processing controls, data input, and system access.

PMIS may identify passenger throughput entries that exceed hourly thresholds for a check lane, but it does not prevent the system from accepting incorrect entries. TSA designates upper limits for passenger check lane throughput, and PMIS notifies a reviewer when an entry exceeds the limit. PMIS does not indicate which lane, hour, or screening equipment exceeded the limit. TSA attempted to demonstrate the review process, but could not determine which entry exceeded the limit. In this case, a reviewer may approve a submission without correcting potential errors. Furthermore, TSA cannot be certain that

[3] *Assessing the Reliability of Computer-Processed Data,* GAO-09-680G, July 2009, www.gao.gov.
[4] TSA classifies its regulated U.S. airports into one of five categories—X, I, II, III, and IV. Category X airports generally have the largest number of passengers boarding planes, and category IV airports have the least.

inaccurate submissions are thoroughly reviewed because PMIS automatically accepts submissions within 48 hours.

PMIS does not have system access controls that prevent unauthorized or accidental changes. In one instance, we identified a checkpoint where PMIS showed AIT throughput that was more than double the total customer throughput at that checkpoint (figure 2). TSA officials explained that a change in PMIS settings resulted in recording inaccurate AIT throughput.

Figure 2: Error on AIT Utilization Report for a Category X Airport

By Checkpoint Performance

Actual - Total AIT Throughput	Target - AIT Throughput	Total Customer Throughput	Actual - % AIT Screened	Target - % AIT Screened	% Effective
4,631	2,108	2,108	219.7%	100.0%	219.7%

Source: TSA.

PMIS Quality Controls

TSA's quality controls for PMIS did not ensure airports submit accurate data to TSA headquarters for reporting the number of passengers screened by AIT. Controls are essential for an agency to achieve effective and efficient program results and safeguard the integrity of their programs. Quality controls include complying with approved policies and procedures, approving and reviewing data, and verifying and reconciling information.

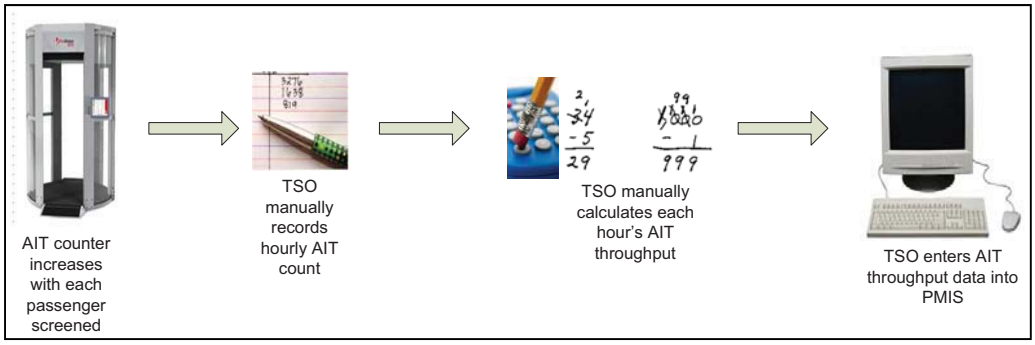
Although TSA has guidance documenting responsibilities for PMIS data entry and review, that guidance does not include procedures for capturing and validating AIT data. TSA's guidance includes the *PMIS Web User Guide* and the *Office of Security Operations Field Guide: Improving Security Effectiveness by Optimizing Utilization of Advanced Imaging Technology*. These documents define PMIS data fields, identify fields requiring data entry, and provide examples of TSA reports on AIT.

TSA did not develop standard procedures or guidance to instruct airports on recording or entering data into PMIS. For example, the five airports visited used different datasheet logs to record AIT throughput. Additionally, these airports did not have a documented procedure for validating AIT throughput data prior to entering the information into PMIS. Without specific procedures on data validation, TSA cannot verify that data entered into PMIS are accurate and reliable.

TSA is unable to assess PMIS data accuracy because it does not require airports to maintain source documents for AIT throughput data. Four of the five airports visited could not immediately provide documentation to validate PMIS data. One airport maintained the original records at each checkpoint for 30 days and then transferred those records to an off-site storage facility. Airport personnel were not able to provide the files quickly when requested because the records were not organized. TSA confirmed it has not tested the accuracy of AIT data in PMIS; instead, it relies on staff experience with throughput data to identify problems with the data.

Airports' manual processes for recording and entering AIT throughput in PMIS may lead to inaccurate information and do not provide an audit trail to validate data accuracy. As illustrated in figure 3, TSOs record passenger throughput using pen and paper, calculate the hourly throughput, and enter the information into PMIS.

Figure 3: Manual Process to Capture Hourly AIT Throughput



Source: OIG analysis of TSA airport process.

We tested a sample of PMIS data for a 10-day period at five category X airports to evaluate data reliability. We were not able to develop a systematic test approach because there were no standard procedures and requirements for the airports to maintain manual records. However, based on this limited testing, we identified the following problems during our data reliability review:

- AIT throughput data recorded in PMIS were different than the source document.
- AIT throughput data on the source document were not recorded in PMIS.
- The starting AIT count was different from the previous day's ending AIT count.
- AIT throughput source documentation was missing.

Without documented procedures standardizing the process to capture AIT throughput and stronger controls to validate AIT data, TSA cannot ensure data in PMIS are accurate and complete. Without reliable throughput data for AIT, TSA decision makers cannot ensure the optimal use of its machines, cannot measure the effectiveness of the technology, and cannot implement improvements in efficiencies.

Recommendations

We recommend that the Deputy Administrator, Transportation Security Administration:

Recommendation #1:

Develop and approve a single, comprehensive deployment strategy that addresses short- and long-term goals for screening equipment.

Recommendation #2:

Develop and implement a disciplined system of internal controls from data entry to reporting to ensure PMIS data integrity.

Management Comments and OIG Analysis

TSA provided comments to the draft of this report. According to its response, TSA agreed with our recommendations. A summary of the responses and our analysis follows. We included a copy of the management comments in their entirety in appendix B.

In its comments, TSA asserted it created an Executive Steering Committee that met weekly to discuss deployment goals and progress; technology development and operational reliability; operator hiring and training progress; operational metrics; Congressional, stakeholder, and international engagements; and opportunities for continuous improvement. However, the results of the steering committee's decisions were not developed into a written baseline to respond to and plan for evolving threats, goals, and priorities. TSA acknowledged the recommendations will help it develop a greater focus on documenting its short- and long-term strategies and improve internal controls relative to data used to influence or inform those strategies.

Response to Recommendation #1: TSA concurred. TSA launched an effort to develop and approve updated deployment strategies that address short- and

long-term goals. The deployment strategies will include Risk Based Security goals and a methodology for assessing the impact of unplanned events.

OIG Analysis: While TSA's actions are responsive to the recommendation, TSA did not provide sufficient detail or a target date for completion of its deployment strategy documents. This recommendation is unresolved and will remain open until TSA provides its approved comprehensive deployment strategy.

Response to Recommendation #2: TSA concurred. TSA agreed that its system can benefit from establishing standard processes and procedures for collecting, calculating, and entering AIT and walkthrough metal detector passenger throughput, as well as developing auditing mechanisms to ensure the processes are followed and TSA can identify and correct incorrect data. TSA noted it was able to both increase the number of AIT deployed and reallocate millimeter wave units to mitigate the removal of backscatter units without degradation in the percent of passengers screened. In addition, TSA asserted PMIS has demonstrated the ability to provide data on AIT utilization.

OIG Analysis: TSA's response to this recommendation does not fully address the intent of the recommendation. Although TSA acknowledged the benefit of establishing standard processes and developing auditing mechanisms for AIT and walkthrough metal detector throughput, the component did not provide specific actions it will take to address the recommendation. The recommendation is unresolved and will remain open until TSA develops and implements internal controls to ensure PMIS data integrity.

Appendix A
Objectives, Scope, and Methodology

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

In response to a congressional request, we audited TSA's deployment and use of AIT. Our audit objective was to determine whether TSA ensured AIT units are being effectively deployed to and fully used in airports. We conducted this audit in response to a request by Representative John Mica, Chairman, Subcommittee on Government Operations, Committee on Oversight and Government Reform. Representative Mica questioned whether TSA was wasting taxpayer dollars by purchasing and deploying AIT units that were not being used.

We reviewed Federal regulations, departmental guidance, and agency procedures for AIT deployment and use, as well as best practices for equipment deployment and data reliability. We reviewed acquisition, deployment, and contract documentation for AIT. We also reviewed TSA guidance on PMIS.

We interviewed TSA headquarters staff responsible for the acquisition, deployment, and use of AIT in the following offices: the Office of Security Capabilities, Office of Security Operations, and the Office of Acquisition. In addition, we interviewed TSA staff responsible for the use of AIT and observed AIT operations at five airports—Chicago O'Hare International Airport, John F. Kennedy International Airport, Lambert-St. Louis International Airport, Newark Liberty International Airport, and Seattle-Tacoma International Airport.

To identify AIT throughput, we extracted PMIS data from TSA headquarters' reporting system to review passenger throughput data from August 1, 2011, through July 31, 2012. We used IDEA software to review the PMIS data for exceptions to TSA's standard throughput rates and to summarize overall AIT usage at TSA's 28 category X airports.

We tested the accuracy of passenger throughput data we extracted from PMIS and concluded the data were of undetermined reliability. We tested PMIS application controls by evaluating data against TSA's standard throughput thresholds and identified instances where values exceeded those limits.

We could not validate PMIS for our proposed timeframe of August 1, 2011, through July 31, 2012, because airports did not retain the records. We requested that the five airports visited maintain and provide source documents for a 10-day period from December 1, 2012, to December 10, 2012. One airport did not comply with the original request so its time period was from January 19, 2013, to January 28, 2013. Our review identified inconsistencies between PMIS and the airports' original source documents.

We conducted this performance audit between May 2012 and May 2013 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards (GAGAS), except that we identified an impairment to our independence in appearance. During this audit, it came to our attention that a family member of a senior OIG official was employed by an entity associated with this audit. To resolve this issue, we employed safeguards to protect the work from the threat to our independence in appearance. Our safeguards included re-evaluating the evidence supporting our findings and conclusions. In our opinion, the impairment to our independence in appearance did not affect the findings and conclusions developed during this audit.

GAGAS requires that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objective, and that the impairment to our independence in appearance did not affect this evidence or any findings and conclusions.

Appendix B
Management Comments to the Draft Report

U.S. Department of Homeland Security
701 South 12th Street
Arlington, VA 20598-6021

Transportation Security Administration

AUG 15 2013

INFORMATION

MEMORANDUM FOR: Anne L. Richards
Assistant Inspector General for Audits
U.S. Department of Homeland Security

FROM: John S. Pistole
Administrator
Transportation Security Administration

SUBJECT: *Transportation Security Administration's Deployment and Use of Advanced Imaging Technology – For Official Use Only OIG Project No. 12-137-AUD-TSA.*

Purpose

This memorandum constitutes the Transportation Security Administration's (TSA) response to the Department of Homeland Security (DHS) Office of the Inspector General (OIG) draft report entitled, *Transportation Security Administration's Deployment and Use of Advanced Imaging Technology – For Official Use Only OIG Project No. 12-137-AUD-TSA.*

Background

The report identifies measures that can be taken by TSA to enhance its deployment and use of Advanced Imaging Technology (AIT). TSA begin deploying AIT in 2007 and accelerated its deployment after the attempted airplane bombing on December 25, 2009. In 2012, Representative John Mica requested that the U.S. Department of Homeland Security (DHS) Office of Inspector General (OIG) conduct an audit to determine whether TSA is effectively deploying AIT and is fully utilizing the equipment at airports.

Discussion

In 2007, TSA conducted a limited acquisition of eight low-rate initial production (LRIP) AITs to determine the applicability of such technology in the checkpoint environment. Based on the success of that initial testing, an additional 35 units were purchased in 2008 and fielded in the secondary position (post-Walk-Through Metal Detector (WTMD) and for secondary screening only) at approximately 19 airports. In 2009, six of the original units were re-configured to the

primary position (co-located with WTMD) to test the feasibility and performance of AIT as a primary screening device. Through data collection efforts during several extended field and laboratory tests, it was determined that AIT would be successful in the primary position for the detection of metallic and non-metallic threats.

After the attempted airplane bombing on December 25, 2009, TSA modified screening procedures to improve the ability to detect explosives hidden in sensitive areas of the body and accelerated AIT deployment. These strategies were intended to improve TSA's ability to detect non-metallic explosives and to increase the use of technology to detect threats concealed on the body in a way that mitigated the need for physical screening procedures. Over the following 3 years, TSA successfully deployed close to 1,000 AIT machines across the system; hiring and training operators, collaborating with internal and external stakeholders to socialize the new security posture, and attending to customer service impacts by a multitude of outreach events and awareness campaigns.

To affect this amount of change in such a short period of time, TSA stood up an Executive Steering Committee that met weekly to discuss the items below and ensure immediate attention to any element of the deployment that presented a risk to the schedule or the efficacy of the effort.

- Deployment goals and progress;
- Technology development, operational reliability;
- Operator hiring and training progress;
- Operational metrics (AIT Throughput, AIT Utilization, Passenger Opt-Outs, etc.);
- Congressional Engagements;
- Stakeholder Engagements (media, passenger services outlets, industry partners, etc.);
- International Engagements; and
- Opportunities for continuous improvement on all fronts

The recommendations in the OIG's report will help TSA to continue developing a greater focus on documenting short- and long-term strategies as well as improving our internal controls relative to data that is used to influence or inform those strategies.

TSA concurs with the recommendations provided by OIG and has already taken steps to address the recommendations. What follows are TSA's specific responses to the recommendations contained in the OIG report.

Recommendation #1: ***Develop and approve a single, comprehensive deployment strategy that addresses short and long-term goals for screening equipment.***

TSA concurs. TSA has already launched the effort to develop and approve updated deployment strategies that address short- and long-term goals. These strategies will include the impact of recent and upcoming Risk Based Security goals as well as provide methodology for assessing impact of unplanned events, such as security-related incidents.

Recommendation #2: ***Develop and implement a disciplined system of internal controls from data entry to reporting to ensure PMIS data integrity.***

TSA concurs. We agree with the recommendation for improving our internal controls for the manual collection, calculation, and data entry of passenger volumes utilizing AIT and WTMD equipment. We agree that the system can benefit from establishing standard processes and procedures for these activities as well as developing auditing mechanisms to ensure they are followed and that incorrect data can be identified and corrected expeditiously.

GAO-09-680G "Assessing Data Reliability" defines risk as "the likelihood that using data of questionable reliability could have substantial negative consequences on the decisions of policymakers and others." Given that authoritative definition, the Office of Security Operations stipulates that TSA was able to increase the total number of deployed AIT to just under 1000 units and increased AIT utilization from about 400,000 passengers per day to over 1,000,000 passengers per day. Using PMIS data in early 2013, TSA was also able to strategically reallocate 129 millimeter wave units to mitigate the required removal of the remaining 171 backscatter (non-Automated Target Recognition enabled) units without degradation in percent of passengers screened. The PMIS application has demonstrated the ability to provide data on AIT utilization. We realize there is always room for improvement to ensure we are collecting the most accurate data possible.

In summary, we concur with the OIG's recommendation. TSA will continue to build on our ability to provide the most accurate data on AIT utilization by working with others internally and externally to improve our internal controls for the manual collection, calculation, and data entry of passenger volumes utilizing our AIT and WTMD equipment.

Appendix C
Major Contributors to This Report

Linda Howard, Director
Christine Haynes, Audit Manager
Tiffany Bellinger, Auditor
Karen Gardner, Auditor
David Lu, Program Analyst
Tessa May-Fraser, Program Analyst
Matthew Noll, Program Analyst
Kevin Dolloson, Communications Analyst
Ralleisha Dean, Independent Report Referencer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Acting Chief Privacy Officer

Transportation Security Administration

Administrator
TSA Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Office of Investigations Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

The OIG seeks to protect the identity of each writer and caller.